IT UNIVERSITY OF COPENHAGEN

DevOps, Software Evolution and Software Maintenance

COURSE CODE: KSDSESM1KU

BACHELOR IN SOFTWARE DEVELOPMENT

DevOps: ITU-MiniTwit

GROUP E — GRL PWR

IT UNIVERSITY OF COPENHAGEN

Name	Email
Andreas Nicolaj Tietgen	anti@itu.dk
Amalie Bøgild Sørensen	abso@itu.dk
My Marie Nordal Jensen	myje@itu.dk

May 9, 2024

2500 words

Table of Contents

1 System Perspective

2 Process Perspective

hallo [1]

3 Lessons Learned

3.1 Lesson 1: Getting Hacked

Just a couple of hours after attending the lecture on security, we got hacked, leading us to experience firsthand how important it is to incorporate security in a CI/CD pipeline.

The first suspicion we got was when we discovered, through our monitoring, that the response time of our server was suddenly very slow. This led us to our Digital Ocean dashboard which showed that the server was using 100% CPU power, which is highly unusual.

From that point the group scoured the server for clues as to what was happening, finding countless calls to `masscan` essentially drowning our server, as well as mysterious installations and what looked like a call to a remote script via a cronjob.

After a few failed attempts to evict the adversary it was decided to destroy the server, as we fortunately had already implemented our Infrastructure as Code, so provisioning and deploying a new server could be done in under half an hour.

After some introspection into our system, we assume that the adversary had gotten access via some ports that we were unaware were exposed. The ports became exposed in an attempt to make the network function between servers in a docker swarm, which seems to override the firewall.

Learning from this, we have worked to close exposed ports from Docker and finding alternative solutions to setting up the network. Another key takeaway is that because we had the necessary monitoring in place, to figure out that the server was being targeted, as well as having our Infrastructure as Code, we were able to detect and react to the attack fairly quickly, giving us only a few hours of downtime.

4 References

[1] Gene Kim. *The DevOPS Handbook - How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. It Revolution Press, 2016. ISBN: 9781942788003.

Appendices